UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/621,258 | 07/15/2003 | Sampo Sovio | 915-007.033 | 9730 |

4955 7590 01/23/2007

WARE FRESSOLA VAN DER SLUYS &
ADOLPHSON, LLP
BRADFORD GREEN, BUILDING 5
755 MAIN STREET, P O BOX 224
MONROE, CT 06468

| EXAMINER | |
|---|---|
| POLTORAK, PIOTR | |
| ART UNIT | PAPER NUMBER |
| 2134 | |

| SHORTENED STATUTORY PERIOD OF RESPONSE | MAIL DATE | DELIVERY MODE |
|---|---|---|
| 3 MONTHS | 01/23/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/621,258 | SOVIO ET AL. | |
| | Examiner | Art Unit | |
| | Peter Poltorak | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *12 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/15/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-27 have been examined.

### *Priority*

2. Acknowledgment is made of applicant's claim for priority based on European Patent Application No. 02015842.4 filed on July 16, 2002.

### *Claim Objections*

3. Claims 1-27 are objected to because of the following informalities: the claim language includes numbers and symbols that seem to aim to clarify the claimed invention (*e.g. "into a first part (d1)" claim 1 or "a password verification value ( )" and "said password verification values (b, ), claim 21*). However, the convention chosen by the applicant does not conform with current U.S. practice. The claim invention should be clearly presented with no need for any additional clues, e.g. referring to drawings.
4. Claims 25-27 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.
5. Claims 25-27 appear to be apparatus claims further limiting the process steps of method claim 1. However, "a delagator" or "a server", recited in claims 25-27 fail to include every feature that they depend on and therefore are improper. As a result, the apparatus claims 25-27 fall to further limit the method claim 1.

   Appropriate correction is required.

### *Claim Rejections - 35 USC § 101*

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 1-27 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 1 for example, recites various operation: splitting a key, forwarding a piece of information or a part of the key, performing some operation on messages etc., but the claim language does not disclose any tangible useful result, i.e. enabling the use of specific resources after successful authorization.

Appropriate correction is required.

### *Claim Rejections - 35 USC § 112*

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 25-27 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Single means claims 25-27, comprise a means recitation that does not appear in combination with another recited element of means. As a result claims 25-27 are

subject to an undue breadth rejection under 35 U.S.C. 112, first paragraph. In re Hyatt, 708 F.2d 712, 714-715, 218 USPQ 195, 197 (Fed. Cir. 1983).

Appropriate correction is required.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1-27 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention.
9. Claims 1-27 suggest "splitting" a key (e.g. master key) into two parts (first and a second part). These two are enable "partial" operation on messages. Although in several places the specification suggest that the word "splitting" should be interpreted similar to dividing (e.g. "The master device 11 further calculates a second half-key d2 as the difference between the available key d and the computed first half-key d1, i.e. d2=d-d1", paragraph 51, or ""In the described embodiment of the invention secret key d is split by the master device into half keys of equal size.", paragraph 84) the examiner was not able to correlate this meaning into the claim language that recites forwarding each of the pieces of a master key (after the splitting) to different devices in order to enable these devices to perform partial secret key operations on messages. Although paragraph 84, for example, does suggest that there is a key d that is a sum of d2 and d1, the examiner is not able to determine (from the specification) at which point this key d is "split". Applicant

should clarify what is considered to be a master key, e.g. key d, that is equal to d2 and d1, and that is split prior to sending partial keys d2 and d1 to separate devices. For purposes of further examination the term "splitting" is treated as best understood.

10. Claim 1-27 are rejected because the preamble of claim 1 does not support the body of the claims. Claim 1 is directed towards "sharing the authorization to use specific resources... accessible via messages on which a secret key operation was applied", but claim 1 falls short of disclosing the actual sharing authentication that allows using specific resources.

Appropriate correction is required.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1, 12-19 and 25-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over APA (Applicant Admitted Prior Art) in view of Stallings (William Stallings, "Cryptography and network security", 2th edition, 1998, ISBN: 0138690170).

As per claim 1 and 25-27, APA discloses splitting a secret master key (d) at a master device into a first part (d1) and a second part (d2), wherein the master device is acting as a delegator of the authorization; forwarding a piece of information to a

slave device acting as a delegatee of the authorization, which piece of information enables the slave device to perform a partial secret key operation on messages based on the first part (d1) of the secret master key (d); and using the second part (d2) of the secret master key to enable the master device to perform a partial secret key operation on messages (m) received from the slave device based on said second part (d2) of said secret master key (d) (APA, the specification last paragraph of pg.1 – first paragraph pg. 2).

12. In APA disclosure it is the master device and not a server that uses the part of the secret master key performing a partial secret key operation on messages received from the slave device. Thus, APA does not disclose "forwarding the second part of the secret master key to a server".

Stallings discloses forwarding the second part of the secret master key to a server (Stallings, "Public-Key Authority pg. 184-185). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to forward the second part of the secret master key to a server as disclosed by Stallings. One of ordinary skill in the art would have been motivated to perform such a modification in order to enable two independent parties to engage in a secure operation.

13. As per claims 12-13, 15 and 17, Stallings' three party exchange (see "Public-Key Authority", pg. 184-185) establishes a confidential channel between the parties allowing secure data transmission and provides security association using cryptographic parameters. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to establish a confidential channel between

the parties allowing secure data transmission and provide security association as disclosed by Stallings given the benefit of providing tighter control over the distribution of secure communication means.

14. Although, as per claims 14 and 16, APA in view of Stallings disclose implementation of the security association an asymmetric algorithm, utilizing symmetric algorithms is an obvious variation that are well known in the art (e.g. Stallings, "2.1 Conventional Encryption Model", pg. 22-23). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement the symmetric algorithm given the benefit of the symmetric algorithms as evidenced by their commercial success.

15. As per claims 18-19, APA in view of Stallings does not disclose forwarding the piece of information or said secret master key only in case the delegator determines that a recipient (the slave device or the server) comprises a tamper resistant certificate indicating that the recipient is compliant with predetermined rights issuer rules. However, Official Notice is taken that it is old and well-known practice to use verify certificates prior to permitting further operation (e.g. U.S. Pub. 20050114666 or using more intuitive example, SSL certificates). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to configure APA in view of Stallings' invention to include forwarding the piece of information or said secret master key only in case the delegator determines that a recipient (the slave device or the server) comprises a tamper resistant certificate indicating that the recipient is

compliant with predetermined rights issuer rules given the benefit of increased security assurance.

16. Claims 2-4, 8-11, 20-24 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over APA (Applicant Admitted Prior Art) in view of Stallings (William Stallings, "Cryptography and network security", 2th edition, 1998, ISBN: 0138690170) and further in view of MacKenzie (MacKenzie and Reiter "Delegation of Cryptographic Servers for Capture-Resilient Devices", Proceedings of the 8th ACM conference on Computer and Communications Security, Pages: 10 - 19, ISBN: 1-58113-385-5, 2001).

Claim 2-4, 8-11, 20-21 and 27 are simply a recursive repetition of APA in view of Stallings.

MacKenzie discloses recursive repletion of splitting a secret key to partial secret keys that are then used in key operations on messages (MacKenzie, "3.4 Delegation protocol", pg. 14-15). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate MacKenzie's recursive mechanism into APA in view of Stallings given the benefit of delegation.

The examiner also points out that the similar to APA's mentioned "Networked cryptographic devices resilient to capture", MacKenzie's discloses using random numbers and a password verification value, transmitting a key computed for a specific delegate once during an initialization process (e.g. MacKenzie "3.2 Device initialization" and "3.3 Signature protocol", pg. 14).

17. As per claim 22, APA in view of Stallings do not disclose verifying an identity of a delegate prior to performing a request. Official Notice is taken that it is old and well-known practice to verify an identity of a requesting parties (e.g. login authentication process or in cryptography verification of challenge request response). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to verify an identity of a delegate prior to perform the delegate request given the benefit of security, in particular in order to avoid potential cryptanalysis.

18. Claims 23-24, certificates are issued by certifying parties. Thus a certificate issued by a certifying party (e.g. delegator to a delegate) reads on a voucher. As a result, claims 23-24 are substantially equivalent to claims 18-19; therefore claim 23-24 similarly rejected.

19. Claims 5-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over APA (Applicant Admitted Prior Art) in view of Stallings (William Stallings, "Cryptography and network security", 2th edition, 1998, ISBN: 0138690170) and MacKenzie (MacKenzie and Reiter "Delegation of Cryptographic Servers for Capture-Resilient Devices", Proceedings of the 8th ACM conference on Computer and Communications Security, Pages: 10 - 19, ISBN: 1-58113-385-5, 2001) and further in view of Pfleeger (Charles P. Pfleeger, "Security in computing", 2nd edition, 1996, ISBN: 0133374866).

20. APA in view of Stallings and further in view of MacKenzie disclose delegation of authorization as disclosed above but fails short of additionally providing restricting bounds policies.

21. However, provide policies, in particular in security area (such as authorization) are well known in the art of information security as illustrated by Pfleeger, for example (Pflegger, pg. 271-276). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to provide restricting bounds policies as taught by Pfleeger given the benefit of ensuring the desired level of a system's security. Furthermore, defining choices of elements used in policies, e.g. "the bounds of the authorization that may be delegated to a delegate or a maximum number of allowed further delegations, would not affect the functionality of the invention as claimed in claim 1. These elements are only found in the nonfunctional descriptive material and do not alter the steps of splitting a key that is then forwarded (according to claim 1) to at least one slave device acting as a delegate. Thus, this descriptive material will not distinguish the claimed invention from the prior art in terms of patentability, see In re Gulack, 703 F.2d 1381, 1385, 217 USPQ 401, 404 (Fed. Cir. 1983); In re Lowry, 32 F.3d 1579, 32 USPQ2d 1031 (Fed. Cir. 1994).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include providing elements of a restricting policy such as the bounds of the authorization that may be delegated to a delegate or maximum number of allowed further delegations because the subjective interpretation of the data does not patentably distinguish the claimed invention.

***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Wack (U.S. Patent No. 7095852) and

Philip MacKenzie and Michael Reiter, "Two-Party Generation of DSA Signatures", Lecture Notes in Computer Science, "Springer Berlin/Heidelberg, ISSN: 0302-9743", 2001.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

1/17/07

KAMBIZ ZAND
PRIMARY EXAMINER